ΟΡΙΣΜΟΣ: Το σύνολο όλων των άρτιων μεταθέσεων καλείται εναλλάσσουσα υποομάδα της Σ_ν με συμβολισμό ως A_ν. (Αποτελεί υποομάδα)

Επίσης, $A_\nu \leq \Sigma_\nu \Rightarrow |A_\nu| = \frac{|\Sigma_\nu|}{2}$

Διότι πχ.

Έστω $A_\nu = \{a_1, \dots, a_k\}$ άρτιες τυχαία αντιμετάθεση $(1,2) = a$

$(1,2) A_\nu = (1,2) \cdot \{a_1, \dots, a_k\} = \{(1,2) a_1, \dots, (1,2) a_k\} \Rightarrow a \cdot a_i = a \cdot a_j$

Μια περιττή f γράφεται άρτια $a f \in A_\nu \Rightarrow a \cdot a f = f$ δίνεται

Άρα το πλήθος των αρτίων = πλήθος των περιττών

Ασκήσεις σελ 44

1) ΜΚΔ $(2,4) \neq 1$ $\mathbb{Z}_8$ όχι κυκλική αν.ν $(p,q) = 1$

7) ΘΔΟ $k\mathbb{Z} \leq \nu\mathbb{Z} \Leftrightarrow \nu / k$

$(\Rightarrow)$ Έστω $k\mathbb{Z} \leq \nu\mathbb{Z} \Rightarrow k\mathbb{Z} \subseteq \nu\mathbb{Z}$ τότε

$k \in k\mathbb{Z} \Rightarrow k \in \nu\mathbb{Z} \Rightarrow k = \nu\mu, \mu \in \mathbb{Z} \Rightarrow \nu / k$

$(\Leftarrow)$: Έστω $\nu / k \Rightarrow (\exists \mu \in \mathbb{Z}) : k = \nu\mu$

$x \in k\mathbb{Z} \Rightarrow x = kz, z \in \mathbb{Z} \Rightarrow x = \nu \cdot (\mu \cdot z) \Rightarrow x \in \nu\mathbb{Z} \Rightarrow k\mathbb{Z} \subseteq \nu\mathbb{Z}$

$k\mathbb{Z} \subseteq \nu\mathbb{Z} \leq \mathbb{Z}$

Αρκεί να ισχύει $k\mathbb{Z} \leq \mathbb{Z}$ που ισχύει πάντα

Αν G ομάδα και $H_2 \subseteq H_1 \leq G$

Για να είναι $H_2 \leq H$ αρκεί $H_2 \leq G$

9) $Y \neq \emptyset$ γιατί $1^\nu = 1 \Rightarrow 1 \in Y$

Έστω $a, b \in Y \Rightarrow a^\nu = 1$ και $b^\nu = 1 \Rightarrow a^\nu \cdot b^\nu = 1 \overset{\text{αβελ.}}{\Rightarrow} (ab)^\nu = 1 \Rightarrow a \cdot b \in Y$

Έστω $a \in Y \Rightarrow a^\nu = 1 \Rightarrow (a^\nu)^{-1} = 1^{-1} \Rightarrow (a^{-1})^\nu \in Y$

16) $G=\left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a,b,c \in \mathbb{Z}_p \right\}$ p πρώτος

$\mathbb{Z}_p = \langle \bar{1} \rangle$

$\langle \bar{0} \rangle, \langle \bar{1} \rangle \leq \mathbb{Z}_p$

$Y_2 = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \, b \in \mathbb{Z}_p \right\}$

$Y_3 = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \, b,c \in \mathbb{Z}_p \right\}$

$Y_4 = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a,b \in \mathbb{Z}_p \right\}$

17) $ab^2 = b^3a$ και $ba^3 = a^2b$ (2)

$\downarrow (\cdot a^2)$

$a^3b^2 = a^2b^3a \overset{(2)}{\Rightarrow} a^3b^2 = b \cdot a^3b^2a \Rightarrow$

$\Rightarrow ba^3b^2 = b^2a^3b^2a \overset{(2)}{\Rightarrow} a^2b^3 = ba^2b^3a \overset{(1)}{\Rightarrow}$

$\Rightarrow ba^3b^2 = ba^2b^3a \Rightarrow$

$\Rightarrow a^2b^2 = ba^2b \overset{(\cdot a^2)}{\Rightarrow} a^4b^2 = a^2ba^2b \overset{(3)}{\Longrightarrow}$

$\Rightarrow ba^6 = a^2ba^2 \Rightarrow ba^4 = a^2b \overset{(3)}{\Rightarrow} a^2ba^4 = ba^6 \Rightarrow$

$\Rightarrow a^2b = ba^2 \overset{(2)}{\underset{ba^3 = ba^2}{\Longrightarrow}} a^3 = a^2 \Rightarrow a = 1$

όπου (3) : $ba^3 = a^2b \Rightarrow a^2ba^3 = ba^6 \Rightarrow \underline{a^4b = ba^6}$ (3)

Εστω πινακας 2x2: $\begin{pmatrix} a & b \\ \gamma & \delta \end{pmatrix}$

ο πινακας $(a) \xmapsto{\text{εμφυτεύεται}} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ ή $\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$

Αρα, μπορουμε:

$$GL(n) \longmapsto GL(n+1)$$

Επισης, γραφαμε

$\Sigma(2) \longmapsto \Sigma(3)$

μεταθ. 2στοιχ μεταθ. 3στοιχ.

$\sigma(1)$	$\sigma(1)$	το $\sigma(1)$ σταθερό
$\sigma(2)$	$\sigma(2)=2$	
$\sigma(3)=3$	$\sigma(3)=\sigma(2)$	

Αρα, $\Sigma_n \longmapsto \Sigma_{n+1}$

σ: αφηνει καποιο απο τα n+1 στοιχεία αναλλοίωτο και αλλάζει τα υπόλοιπα

ΠΡΟΤΑΣΗ: Εστω $X \subseteq O$, O ομάδα.
Υπαρχει $Y(x) \leq O$ που περιέχει τα λιγότερα στοιχεία και εχει το X υποσυνολο $Y(x) = \bigcap A \leq O$ και $Y(x) \supseteq X$
$A \leq O$
$X \subseteq A$
Το $Y(x)$ αποτελείται από πεπερασμενα γινόμενα στοιχείων του X και των αντιστροφων του (οι επαναλήψεις επιτρέπονται)
$x_i \in X \Rightarrow \underbrace{x_i x_i \dots x_i}_{\kappa\ \varphi o\rho.} \in Y(x)$

ΟΡΙΣΜΟΣ: Εστω $X \subseteq O$, O ομαδα και $Y(x)$ η τομή ολων των υποομάδων που περιέχουν το X. Η $Y(x)$ γεννάται απο το X ή το X συνολο γεννητόρων.

ΠΑΡΑΤΗΡΗΣΗ: Μας ενδιαφέρει το X να έχει τον ελάχιστο αριθμό στοιχείων

πχ

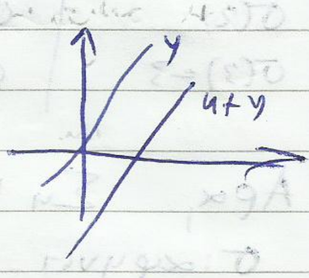
- $\mathbb{Z}_n = \langle a \rangle$, $(a,n)=1$
Ένας γεννήτορας
- Αλλά, στο $\mathbb{Z}_n \times \mathbb{Z}_k$ = Δύο γεννήτορες με $(n,k)\neq 1$
- Η Σ_3 δύο γεννήτορες f,g με $f^3=1=g^2$ και $gfg^{-1}=f^{-1}$
- Η D_n δύο γεννήτορες

ΣΥΜΠΛΟΚΑ

Έστω ομάδα G και υποομάδα της Y

Πιο γενικά έστω V διαν. χώρος

και $Y \le V \Rightarrow u+Y$ δεν είναι υπόχωρος



Για κάθε $a \in G$ ορίζεται το σύμπλοκο

αριστερό σύμπλοκο: $aY = \{ab \mid b \in Y\}$

δεξιό σύμπλοκο: $Ya = \{ba \mid b \in Y\}$

όχι υποομάδες

Πχ

$\nu\mathbb{Z} \le \mathbb{Z}$, $\nu \in \mathbb{N}$

$m+\nu\mathbb{Z} = \{m+\nu k \mid k \in \mathbb{Z}\} = u+\nu\mathbb{Z} = \bar{u}$

Αν $m \ge \nu \Rightarrow m = \pi\nu + u$, $0 \le u < \nu$

όλα τα σύμπλοκα του $\mathbb{Z}$ ως προς $\nu\mathbb{Z}$ είναι τα

$\{\bar{0}, \bar{1}, \dots, \overline{(\nu-1)}\} = \mathbb{Z}_\nu$

Έχουν οριστεί μέσω σχέσης ισοδυναμίας

Ορίζουμε ένα σχέση $a \Sigma \gamma \Leftrightarrow a\gamma^{-1} \in Y$ με $Y \le G$ και $a, \gamma \in G$

$a \Sigma b \Leftrightarrow a-b$ διαιρ. του $\nu \Rightarrow \nu | a-b \Leftrightarrow a-b \in \nu\mathbb{Z}$

ΠΡΟΤΑΣΗ: Αν $Y \leq O$ υποομάδα τότε η σχέση
$a \Sigma \gamma \Leftrightarrow a\gamma^{-1} \in Y$ είναι σχέση ισοδυναμίας
Απόδειξη:

$\gamma \Sigma a \Rightarrow \gamma a^{-1} \in Y \Rightarrow \exists z \in Y : z = \gamma a^{-1} \Rightarrow \gamma = za \in Ya$

$u + \nu\mathbb{Z} = \overline{u}$

κλάσεις ισοδυναμίας aY με $a \in O$
$\{ aY \mid a \in O \}$
$a = e \Rightarrow eY = Y = zY, \forall z \in Y = Yz, \forall z \in Y$
επίσης μπορεί να έχουμε
$aY = bY \Leftrightarrow Y = a^{-1}b \cdot Y \Rightarrow a^{-1}b \in Y$ ή $b^{-1}a \in Y$

ΙΔΙΟΤΗΤΕΣ
1) $Ya = Yb \Leftrightarrow ab^{-1} \in Y$ ή $ba^{-1} \in Y$
2) $Ya \cap Yb = \emptyset$ ή $Ya = Yb$
3) Αν $Ya \neq Yb \Rightarrow |Ya| = |Yb|$ πλήθος στοιχείων
4) Όσα αριστερά σύμπλοκα έχει η O, τόσα έχει και η δεξιά

ΑΠΟΔΕΙΞΗ:
3) Αρκεί $|Ya| = |Y|$
Ορίζουμε την $\phi : Y \to Ya$ με $\phi(z) = za$
Η ϕ: 1-1 $za = z'a \Rightarrow z = z'$ γιατί ο ομάδα
Η ϕ επί $\forall za, \exists z'$ με $\phi(z') = z'a = za \Rightarrow$
$\Rightarrow z = z'$

4) $L_Y(O) = \{$ αριστ. σύμπλοκα $\} = \{ aY \mid a \in O \}$
$R_Y(O) = \{$ δεξ. σύμπλοκα $\} = \{ Yb \mid b \in O \}$
Μέσω αντιστροφής $aY \to (aY)^{-1} = Ya^{-1}$. Το αριστερό έγινε δεξί

Ασκήσεις

σελ. 58 1, 2, 3, 4, 5, 6, 7

σελ 67 1, 2, 4, 6.

ΟΡΙΣΜΟΣ: Έστω $Y \leq O$

Επειδή το πλήθος των αριστερών συμπλόκων ισούται με το πλήθος των δεξιών, ορίζεται ο δείκτης της Y στην O με $|O:Y|$ = πλήθος συμπλόκων

ΠΟΡΙΣΜΑ: Έστω $Y \leq O$ και $|O:Y|$ δείκτης της Y στον O

Υποθέτουμε $|O| < \infty$. $|O| = |Y| \cdot |O:Y|$ [Θεώρημα Lagrange]

Απόδειξη

Τα σύμπλοκα διαμερίζουν την O

Άρα $|O|$ = το άθροισμα του πλήθους των συμπλόκων $= |Y| \cdot |O:Y|$

$|a_i Y| = |a_j Y|$

$O = \bigcup_{i=1}^{k} a_i Y \Rightarrow |O| = \sum_{i=1}^{k} |a_i Y| = n|Y| = |O:Y| \cdot |Y|$

ΠΟΡΙΣΜΑ: Αν $|O| < \infty$ και $Y \leq O \Rightarrow$

$\Rightarrow |Y| / |O|$ και $a^{|O|} = e$ $\forall a \in O$

ΘΕΩΡΗΜΑ (Lagrange)

Αν $|O| < \infty$ και η τάξη της είναι πρώτος αριθμός τότε αυτή είναι κυκλική

Αποδ.

Αν $O \neq \langle a \rangle \Rightarrow \exists b \in O$ και $b \notin \langle a \rangle$

$|\langle b \rangle| < |O|$ και $|\langle b \rangle| / |O|$ αδύνατο

($\not\Leftarrow$) πχ

$|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4 / 4$

Πχ1

$\Sigma_3 = \{1, f, f^2, g, fg, f^2g\}$

$Y = \langle f \rangle$ κυκλικόν

Θα είναι σε πλήθος: $\dfrac{6}{|Y|} = \dfrac{6}{3} = 2$

$eY = Y$ βασικό σύμπλοκο

$g \notin Y \Rightarrow gY$, Άρα $\Sigma_3 = Y \sqcup gY$

Πχ2

$Z = \langle g \rangle \Rightarrow$ πλήθος $= |\Sigma_3 : Z| = \dfrac{6}{|Z|} = \dfrac{6}{2} = 3$

βασικό $Z = \{1, g\}$
$f \in \sigma - Z \Rightarrow fZ = \{f, fg\}$
και
$f^2 \in \sigma - Z - fZ \Rightarrow f^2Z = \{f^2, f^2g\}$

ΠΡΟΤΑΣΗ: Το σύνολο $\mathbb{Z}_\nu^* = \mathbb{Z}_\nu - \{\bar{0}\}$ αποτελεί πολ/στική ομάδα $\Leftrightarrow$ ν πρώτος.

Απόδ.
$\mathbb{Z}_\nu^*$ ομάδα $\Leftrightarrow$ κλειστό ως προς το γινόμενο
Έστω a, b με $0 < a, b < \nu$
$\bar{a} \cdot \bar{b} = \overline{a \cdot b} \neq \bar{0} \Leftrightarrow (a, \nu) = 1 \wedge (b, \nu) = 1$
Δηλ. αν $1 < a < \nu$ τότε $(a, \nu) = 1 \Rightarrow$ ο ν δεν έχει μικρότερους διαιρέτες εκτός από το 1. Άρα ν πρώτος
Αλλά όταν $(a, \nu) = 1 \Rightarrow (\exists a^{-1} \in \mathbb{Z}_\nu)$

ΘΕΩΡΗΜΑ (fermat)

Αν p πρώτος και a δεν διαιρείται απο τον p τοτε $a^{p-1} \equiv 1 \bmod p$

Αποδ.

$|\mathbb{Z}_p^*| = p-1 \Rightarrow \forall \bar{a} \in \mathbb{Z}_p^* : a^{p-1} \equiv 1 \bmod p$

Αν $a > p \Rightarrow a^{p-1} \equiv (a \bmod p)^{p-1} = v^{p-1} \bmod p = 1 \bmod p$

$v = a - kp$ και

$0 < v < p$

Εστω v οχι απαραίτητα πρώτος $\mathbb{Z}_v^*$ οχι ομάδα απαραίτητα

Εστω $A = \{ b / 0 < b < v$ και $(b, v) = 1\}$

$A \subset \mathbb{Z}_v^*$

Αν $b, b' \in A \Rightarrow bb' \in A$ διότι

αν $(bb', v) = d > 1 \Rightarrow \exists p$ πρωτ με $p | bb'$ και $p | v$. Αρα, $p | b$ και $p | v \Rightarrow (b, v) = kp$ Ατοπο

Η πράξη στο A είναι Κ.Ο.

Για τον αντίστροφο:

$\forall b \in A \Rightarrow \exists b^{-1} \in A$

$b \in A \Rightarrow (b, v) = 1 \overset{Bezout}{\Rightarrow} bx + vy = 1 \quad x, y \in \mathbb{Z}$

$(bx + vy = 1) \bmod v \Rightarrow bx = 1 \bmod v \Rightarrow$

$\Rightarrow \exists x \bmod v$ με $(x \bmod v) = b^{-1} \bmod v$

Αρα, A ομάδα

$|A| = \varphi(v)$ - Συνάρτηση του Euler

ΘΕΩΡΗΜΑ (EULER) Αν $(a, v) = 1$ τοτε είναι $a^{\varphi(v)} = 1 \bmod v$

ΘΕΩΡΗΜΑ

Εστω p πρωτος τοτε $\mathbb{Z}_p^*$ κυκλική